UNCLASSIFIED

30 November 2015

NORTH DAKOTA

HOMELAND SECURITY

Cyber Summary

The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Table of Contents

North Dakota

Nothing Significant to Report

Regional

Nothing Significant to Report

National

Nothing Significant to Report

International

(International) **State-sponsored cyberspies inject victim profiling and tracking scripts in strategic websites.** Security researchers from FireEye discovered an attack campaign dubbed WITCHCOVEN, which has injected computers profiling and tracking scripts into over 100 Web sites involved in international business travel, diplomacy, energy production and policy, international economics, and official government work. The malware was designed to identify users of interest and target such users with exploits designed for their specific computer and software configurations.
http://www.computerworld.com/article/3005270/malware-vulnerabilities/state-sponsored-cyberspies-inject-victim-profiling-and-tracking-scripts-in-strategic-websites.html#tk.rss_security

(International) **A quarter of web-accessible devices have vulnerable firmware.** Researchers from EURECOM and Ruhr University in Bochum, Germany, released a study confirming the weak state of security for Internet of Things (IoT) devices included cross-site scripting (XSS) vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, SQL injection (SQLi) vulnerabilities, and remote code/command

execution (RCE) vulnerabilities which can grant attackers access to devices, spy on users, steal data, and rewrite the firmware to perform other malicious activities. http://news.softpedia.com/news/a-quarter-of-web-accessible-devices-have-vulnerable-firmware-496229.shtml

(International) 15-year-old Brit charged with DDoS attacks, bomb threats. British police arrested and charged a 15-year-old teenager November 16 for violating the Computer Misuse Act and Criminal Law Act after he launched a series of Distributed Denial of Service (DDoS) attacks from his home targeting companies and servers in Africa, Asia, Europe, and North America, as well as delivering several bomb threats against North American airlines via social media platforms. http://news.softpedia.com/news/15-year-old-brit-charged-for-ddos-attacks-bomb-threats-496420.shtml

(International) Dell security error widens as researchers dig deeper. Researchers from Duo Security discovered that new Dell laptops were found with a self-signed root digital certificate, eDellRoot, which can allow attackers to conduct a man-in-the-middle attack, spy on incoming data, and use private keys to create their own digital certificates to produce fake Web sites that appear legitimate. Dell Inc. reported they plan to release instructions on how to remove the certificates. http://www.computerworld.com/article/3008077/security/dell-security-error-widens-as-researchers-dig-deeper.html#tk.rss_security

(International) ISIS retaliates against Anonymous, leaks data of "To-be-killed" US officials. Hackers from the Islamic State Hacking Division leaked a list containing data about employees who served on bases located in the Middle East, including personnel from the U.S. Defense Intelligence Agency, the FBI, the CIA, and the National Counterterrorism Center, the U.S. National Guard, and other Federal government agencies, via a Twitter account. The leak was contained. http://news.softpedia.com/news/isis-retaliates-against-anonymous-leaks-data-of-to-be-killed-us-officials-496593.shtml

Banking and Finance Industry

(National) PoS malware spread via weaponized Microsoft Word documents. Researchers from Proofpoint discovered the point-of-sale (PoS) malware dubbed

AbaddonPOS was a part of a malware-delivery campaign allowing attackers to download other malware from Command and Control servers (C&C) using its own custom protocol via Microsoft Word documents and malicious Web sites, in an attempt to steal credit and debit card transaction data. http://news.softpedia.com/news/pos-malware-spread-via-weaponized-microsoft-word-documents-496155.shtml

(International) New Dyre variant can target Windows 10 and Microsoft Edge users. Security researchers from Heimdal discovered a new version of Dyre/Dyreza banking malware that can compromise a variety of Windows systems, connect into various browsers including Google Chrome and Internet Explorer, and terminate security software processes via a disguised Upatre trojan sent through spam emails that allows attackers to inject additional malware once the computer system has been compromised. http://www.net-security.org/malware_news.php?id=3156

(International) ModPOS is a sophisticated criminal malware framework targeting POS devices. Security specialists from iSIGHT Partners discovered November 24 a new complex form of malware called ModPOS that targets U.S. retailers' point-of-sale (PoS) systems via its three modules including Uploader/Downloader, Keylogger, and POS Scrapper that use obfuscation and encryption to evade security software and use its command and control (C&C) server to instruct the infected device to fetch other modules, once the stolen information is deemed valuable. http://news.softpedia.com/news/modpos-is-a-sophisticated-criminal-malware-framework-targeting-pos-devices-496643.shtml

(International) Researcher creates gadget that bypasses credit card chip&PIN safeguards. A researcher created MagSpoof, a device that can accurately read and predict credit card numbers and bypass chip&PIN (CnP) safeguards by using information stored inside the magstripe (magnetic strip), which can be extracted. Data is removed and fed to MagSpoof allowing hackers to make financial transactions by placing the device near point-of-sale (PoS) systems. http://news.softpedia.com/news/researcher-creates-gadget-that-bypasses-credit-card-chip-pin-safeguards-496697.shtml

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(National) Starwood warns of data breach at 54 of its hotels. Connecticut-based Starwood Hotels & Resorts Worldwide Inc., reported November 22 that its payment systems were compromised at 54 of its hotel restaurants, gift shops, and other retail areas after malware was found in its systems that allowed attackers access to debit and credit card information including names, card numbers, security codes, and expiration dates of customers. The malware infected computer systems as early as November 2014 and has been removed. http://wwlp.com/2015/11/22/starwood-warns-of-data-breach-at-54-of-its-hotels/

(Wisconsin) Wilderness resort reports credit card data breach. Wisconsin Dells officials reported November 23 that its Wilderness Resort's point-of-sale (PoS) system for processing credit and debit card transactions was compromised and may affect guests with reservations from March 9 – June 8 after a malware was found in its systems. The malware was removed and the resort is offering one year of free credit monitoring to guests who may have been affected. http://www.jsonline.com/business/wilderness-resort-reports-credit-card-data-breach-b99621592z1-353041801.html

(National) Hilton Hotels hit by cyberattack. Hilton Worldwide Holdings, Inc. officials reported November 24 that its point-of-sale (PoS) computer systems were breached via a malicious code that collected and stole credit card information including names, card numbers, security codes, and expiration dates. Hilton is investigating the breach and advised customers to monitor their bank accounts for fraudulent activities. http://www.securityweek.com/hilton-hotels-hit-cyber-attack

Communications Sector

Nothing Significant to Report

Critical Manufacturing

(International) Backdoor within backdoor puts over 600,000 Arris cable modems in danger. A Brazilian security researcher discovered that over 600,000 Arris' old cable modems, TG862A, TG862G, DG860A, were manufactured with 2 backdoor codes installed in its hardware that can be activated via the libarris_password.so library, and if exploited, enables attackers to access the modem and enable Secure Shell (SSH) or Telnet ports, to access a BusyBox shell. http://news.softpedia.com/news/backdoor-within-backdoor-puts-over-600-000-arris-cable-modems-in-danger-496485.shtml

(International) Reuse of Cryptographic keys exposes millions of IoT: study. Researchers from SEC Consult released a report identifying that millions of Internet-of-Things (IoT) devices use the same cryptographic keys hardcoded into the firmware, including secure shell (SSH) host keys and X.509 certificates used for Hypertext Transfer Protocol Secure (HTTPS), that may allow attackers to obtain sensitive information by connecting to a victim's network and leveraging the keys to launch impersonations, man-in-the-middle (MitM) attacks, and passive decryption attacks. http://www.securityweek.com/reuse-cryptographic-keys-exposes-millions-iot-devices-study

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(National) Police body cameras shipped with pre-installed Conficker virus. iPower Technologies found that body cameras sold to police forces around the

U.S. were pre-infected with the Conficker worm (Win32/Conficker.B!inf.), which was discovered in the device's internal drive and records data that can be downloaded onto a computer via Universal Serial Bus (USB) cable. Researchers attempted to notify Martel Electronics, the company that sells the body cameras. http://news.softpedia.com/news/police-body-cameras-shipped-with-pre-installed-conficker-virus-496177.shtml

Energy

(International) Oil and gas companies indirectly put at risk by vulnerabilities in ERP systems. Researchers from ERPScan presenting at Black Hat Europe 2015 showed how a vulnerability in an enterprise resource planning (ERP) suite from SAP and Oracle used inside oil and gas companies, could allow an attacker to gain access into operation technology (OT) infrastructure through connected applications that are insecure. The researchers also determined that misconfigurations, the presence of unnecessary privileges, and custom code provided entry or access escalation points for attacks. http://news.softpedia.com/news/oil-and-gas-companies-indirectly-put-at-risk-by-vulnerabilities-in-erp-systems-496124.shtml

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(National) OPM's $20 million contract for post-hack ID protection violated federal contracting rules. The inspector general of the U.S. Office of Personnel Management announced November 12 that a $20 million contract to offer identity theft protection to some 4.2 million Federal employees who had their personal information hacked violated the Federal Acquisition Regulations and the

agency's own policies after it was awarded. Investigators found significant deficiencies in the contract award process. http://www.nextgov.com/cybersecurity/2015/11/opms-20-million-contract-post-hack-id-protection-violated-federal-contracting-rules/123649/

(Georgia) Data breach in Georgia could affect 6 million voters. The Georgia Secretary of State announced November 18 that approximately 6.2 million registered voters may have had their Social Security numbers and personal identifying information illegally disclosed October 13 after the secretary's office inadvertently sent the information to 12 organizations who subscribe to voter lists maintained by the State. An investigation into the incident is ongoing. http://www.myajc.com/news/news/state-regional-govt-politics/data-breach-in-georgia-could-affect-6-million-vote/npQj8/

(National) DHS runs many unsecured databases: IG. The DHS Inspector General released a report November 13 that found several vulnerabilities in DHS databases due to unpatched systems, including classified networks that could potentially allow an attacker to exploit the vulnerabilities and gain access into data. The report also found that the agency did not include classified system information on its monthly scorecard, in addition to inaccurate or incomplete information in management systems, among other security gaps. http://www.homelandsecuritynewswire.com/dr20151123-dhs-runs-many-unsecured-databases-ig

Information Technology and Telecommunications

(International) Thousands of sites infected with Linux encryption ransomware. Researchers from Dr. Web reported that approximately 2,000 Web sites were compromised by the Linux file-encrypting ransomware dubbed Linux.Encoder1, that targets the root and home files, web servers, backups, and source code via a downloaded file containing the public RSA key used to store AES keys that adds .encrypt extension to each file, allowing files to be nearly impossible to recover without paying a ransom to the attackers. A patch was released, but experts warned that attackers may update the malware to make file decryption more difficult. http://www.securityweek.com/thousands-sites-infected-linux-encryption-ransomware

(International) Compromised Web site fools security vendor, continues to infect users. Researchers from Palo Alto Networks reported that the CryptoWall 3.0 ransomware, that previously affected all users via the Angler Exploit Kit when users visited the Web site, cxda.[.]gov[.]cn, was still active and compromised 4,000 additional Web sites despite initial reports that revealed the malicious campaign had stopped. Researchers revealed a "dormant" and "filtering" functionality imbedded in the campaign's malicious code allowed attackers to go unnoticed depending on the Web sites' source Internet Protocol (IP) and user agent.
http://news.softpedia.com/news/compromised-website-fools-security-vendor-continues-to-infect-users-496178.shtml

(International) Flaw in D-Link switches exposes corporate networks: Researchers. Security researchers from Elastica's Cloud Threat Labs discovered a flaw in DGS-1210 Series Gigabit Smart Switches from D-Link that can be exploited by remote attackers to access backup files found on the flash memory and the web server, where log and configuration files are stored, with any authentication credentials if the attackers identify the targeted device's Internet Protocol (IP) address.
http://www.securityweek.com/flaw-d-link-switches-exposes-corporate-networks-researchers

(International) Cyber crooks actively hijacking servers with unpatched vBulletin installations. Symantec researchers discovered that attackers are using a patched zero-day flaw that affects vBulletin Connect versions 5.1.4 through 5.1.9, to remotely execute code on a vulnerable server by first downloading and executing a multipurpose malicious shell script, filesender1.sh onto a vulnerable server via a single Hypertext Transfer Protocol (HTTP) request.
http://www.net-security.org/secworld.php?id=19113

(International) Automation fuels onslaught of web app attacks: Report. Imperva released its Web Application Attack Report (WAAR) revealing that more than 75 percent of analyzed applications were targeted by automated attacks via SQL injection (SQLi), remote file inclusion (RFI), remote code execution (RCE), directory traversal (DT), cross-site scripting (XSS), spam, file upload (FU), and Hypertext Transfer Protocol (HTTP) reconnaissance, to compromise users and

steal sensitive information as cybercriminals leverage automated tools, making SQL injections attacks 3 times higher this year than previous years. http://www.securityweek.com/automation-fuels-onslaught-web-app-attacks-report

(International) Security flaws in LastPass exposed user passwords. LastPass security team released patches addressing a series of bugs and design flaws, discovered by two researchers from Salesforce, that could have been used to exploit user passwords through an attack against LastPass via various vectors including a special disable one-time password (dOTP) that can be used for authentication to access the encrypted vault key and decrypt it, and bypass IP restrictions and two-factor authentication (2FA), as well as using custom_js to inject and execute JavaScript code on login pages of Web sites. http://www.securityweek.com/security-flaws-lastpass-exposed-user-passwords

(International) Data breach at biz that manages Cisco, F5, Microsoft certifications. The certification management provider, Pearson VUE reported that its Credential Manager (PCM) system was breached, allowing attackers to access Cisco certification users' information including their names, mailing address, email address, and phone numbers. Pearson reportedly believes Social Security numbers were not disclosed and other PCM systems were not compromised. http://www.theregister.co.uk/2015/11/23/pearson_vue_data_breach_pcm/

(International) Nmap 7 brings faster scans, other improvements. Network Mapper (Nmap) released its Nmap Security Scanner 7.0.0 addressing significant improvements including the Nmap Scripting Engine (NSE) that allows users to construct script designed to automate networking tasks, an improved Internet Protocol version 6 (IPv6) support, faster and improved Secure Sockets Layer (SSL) and Transport Layer Security (TLS)-related scans, and an updated version of its Ncat utility. http://www.securityweek.com/nmap-7-brings-faster-scans-other-improvements

(International) Researchers find multiple Chrome extensions secretly tracking users. Researchers from Detectify Labs discovered that Google Chrome extensions including HooverZoom, SpeakIt, ProxFlow, Instant Translate, and other extensions were embedded with an analytics code to track users' browsing history, collect data from cookies, and view secret access tokens from Facebook

Connect without users' consent while surfing across Web sites in different browser tabs. http://news.softpedia.com/news/researchers-find-multiple-chrome-extensions-secretly-tracking-users-496596.shtml

(International) VPN vulnerability "Port Fail" reveals user's real IP address. Network security experts from Perfect Privacy discovered a vulnerability in virtual private network (VPN) providers' internal routing table and port forwarding settings, which can allow an attacker to learn a victim's real Internet Protocol (IP) address by directing victims to access a resource (image embedded on a site) hosted on the same VPN server. http://news.softpedia.com/news/vpn-vulnerability-port-fail-reveals-user-s-real-ip-address-496808.shtml

US-CERT Updates and Vulnerabilities

IRS Releases First in a Series of Tax Security Tips Published November 27, 2015
The Internal Revenue Service (IRS) has released the first in a series of tips intended to increase public awareness of how to protect personal and financial data online and at home. A new tip will be available each Monday through the start of the tax season in January, and will continue through the April tax deadline.
The first tip focuses on seven simple steps to secure your computer when conducting business online. US-CERT encourages users and administrators to review IRS Security Awareness Tax Tip Number 1 for additional information.
Read Full Entry »

US-CERT Alerts Users to Holiday Phishing Scams and Malware Campaigns
Published November 25, 2015 | Last revised November 27, 2015
US-CERT reminds users to remain vigilant when browsing or shopping online this holiday season. Ecards from unknown senders may contain malicious links. Fake advertisements or shipping notifications may deliver infected attachments. Spoofed email messages and fraudulent posts on social networking sites may request support for phony causes.

To avoid seasonal campaigns that could result in security breaches, identity theft, or financial loss, users are encouraged to take the following actions:
Read Full Entry »

Dell Computers Contain CA Root Certificate Vulnerability

Published November 24, 2015 | Last revised November 27, 2015
Dell personal computers using the preinstalled certificate authority (CA) root certificate (eDellRoot) contain a critical vulnerability. Exploitation of the vulnerability could allow a remote attacker to read encrypted web browser traffic (HTTPS), impersonate (spoof) any website, or perform other attacks on the affected system.
The eDellRoot certificate originated from an update to the Dell Foundation Services (DFS) application on August 18, 2015. As of November 23, that update is no longer being provided. The certificate was also preinstalled on some systems November 20–23, 2015. Dell is pushing a DFS software update to remove the vulnerable certificate from affected systems.
US-CERT encourages users and administrators to review Vulnerability Note VU#870761 and Dell's blog post (link is external) for more information and guidance on removing the certificate.
Read Full Entry »

VMware Releases Security Updates

Published November 19, 2015
VMware has released security updates to address a vulnerability in vCenter, vCloud Director, and Horizon View. Exploitation of this vulnerability may allow an attacker to obtain sensitive information.
Users and administrators are encouraged to review VMware Security Advisory VMSA-2015-0008 (link is external) and apply the necessary updates.
Read Full Entry »

IC3 Warns of Cyber Attacks Focused on Law Enforcement and Public Officials

Published November 18, 2015

The Internet Crime Complaint Center (IC3) has issued an alert warning that law enforcement personnel and public officials may be at an increased risk of cyber attacks. In addition to doxing (the act of gathering and publishing individuals' personal information without permission), threat actors have been observed compromising the email accounts of officers and officials. These target groups should protect their online presence and exposure.
Users are encouraged to review the IC3 Alert for details and recommended security measures. Refer to US-CERT Tip ST06-003 for information on staying safe on social networking sites.
Read Full Entry »

Adobe Releases Security Updates for ColdFusion, LiveCycle Data Services, and Adobe Premiere Clip Published November 17, 2015
Adobe has released security updates to address multiple vulnerabilities in ColdFusion, LiveCycle Data Services, and Adobe Premiere Clip. Exploitation of some of these vulnerabilities may allow a remote attacker to take control of an affected system.
Users and administrators are encouraged to review Adobe Security Bulletins for ColdFusion (link is external), LiveCycle Data Services (link is external), and Adobe Premier Clip (link is external) and apply the necessary updates.

ICS-Cert Alerts & Advisories

Nothing Significant to Report

Public Health

(Illinois) Illinois data breach; agency posts personal information on public website. The Illinois Department of Insurance will notify an unknown amount of individuals after the department inadvertently sent filings from Blue Cross Blue Shield to the System for Electronic Rate and Form Filing (SERFF) database, which posted the information on its publicly available Web site. The department is

taking steps to prevent future disclosures after receiving a complaint that Social Security numbers from Blue Cross Blue Shield could be seen. http://kwqc.com/2015/11/13/illinois-data-breach-agency-posts-personal-information-on-public-website/

Transportation

(National) United Airlines patches serious flaw after 6 months. United Airlines patched a vulnerability in its MileagePlus mobile app after a researcher determined that an attacker could gain access to MileagePlus accounts and user information through an insecure direct object references (IDOR) vulnerability discovered when the researcher changed one of the parameters in mpNumber, which is likely the MileagePlus number. http://www.securityweek.com/united-airlines-patches-serious-flaw-after-6-months

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165